UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* SUBJECT DEVICES 1-4	)	Case No. MJ25-127

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SUBJECT DEVICES 1-4, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(4)(B), (b)(2)	Possession of Child Pornography

The application is based on these facts:

✓ See Affidavit of SA Daniel Orlando, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

DANIEL A ORLANDO Digitally signed by DANIEL A ORLANDO Date: 2025.03.09 12:16:50 -07'00'

Applicant's signature

Daniel A. Orlando, Special Agent

Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/11/2025

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Special Agent Daniel A. Orlando, being first duly sworn on oath, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2022, and am currently assigned to the HSI Resident Agent in Charge (RAC) Tacoma Office. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)(A)) in all forms of media including computer media.

2. Prior to my commission as a SA with HSI, I was a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) and had served in that capacity since April of 2019. During my tenure with the FBI, I investigated criminal enterprises, narcotics, violent crime, gang activity, and worked with and alongside the FBI Violent Crimes Against Children (VCAC) investigative group in that office. Aside from my commission as an FBI TFO, I was employed as a Deputy Sheriff and Detective in Central Florida and had been employed as such since 2009. I have participated as a case agent, co-case agent, undercover, and investigative agent in child exploitations, gang related, violent crime, narcotics, and other investigations.

3. I have also been the affiant on numerous arrest warrants, search warrants, and court orders at the Federal and State level. Over the last approximately 16 years as a sworn law enforcement officer, I have received extensive training and experience

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

concerning investigations of federal and state violations of law. In connections with my duties and responsibilities as an HSI Special Agent, FBI TFO, and Detective, I have testified in federal and state judicial proceedings and prosecutions for violations of federal and state law. As an HSI Special Agent, I have received extensive training in a variety of investigative and legal matters of violations of federal and state law. I have participated in numerous Child Exploitation investigations as the primary investigator or in a subsidiary role. I have received training regarding investigations of Child Sexual Abuse Material (CSAM)[1] and Child Exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter.

IDENTIFICATION OF THE SUBJECT DEVICES TO BE EXAMINED

5. This Affidavit is submitted in support of an application to search the following digital devices (hereinafter "the SUBJECT DEVICES"), as further described in Attachment A, for evidence, fruits and instrumentalities, as further described in Attachment B, of violation 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), the TARGET OFFENSE.

> One grey Samsung Galaxy S23 FE 128GB, identified by model name: SM-S711U (**SUBJECT DEVICE 1**), currently in the possession of Homeland Security Investigations.

[1] In this affidavit, I am using CSAM and child pornography, as defined by 18 U.S.C. § 2256, interchangeably.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

One teal Samsung Galaxy A73, identified by model name: SM-A736B/DS (**SUBJECT DEVICE 2**), currently in the possession of Homeland Security Investigations.

One grey HP Laptop, identified by serial number 5CG0383K3W (**SUBJECT DEVICE 3)**, currently in the possession of Homeland Security Investigations.

One Dark grey/black Alienware Laptop, identified by service tag number/serial number HCSVTP2 (**SUBJECT DEVICE 4**), currently in the possession of Homeland Security Investigations.

(The listed items together will be hereinafter referred to as **SUBJECT DEVICES)**

SOURCES OF INFORMATION

6. I have obtained the facts set forth in this Affidavit through my personal participation in the investigation described below; from oral and written reports of other law enforcement officers; and from records, documents and other evidence obtained during this investigation. Insofar as I have included event times in this affidavit, those event times are approximate.

7. Since this affidavit is being submitted for the limited purpose of obtaining authority to search the SUBJECT DEVICES, I have not included every fact known concerning this investigation. I have set forth only the facts that I believe are essential for a fair determination of probable cause.

SUMMARY OF THE INVESTIGATION

8. On March 2, 2025, United States citizen Sean Henry KOOREN, sought entry into the United States at Seattle-Tacoma International Airport in Seattle, Washington from a flight returning from Ninoy Aquino International Airport in Manila, Philippines where he had been visiting for approximately (3) months. KOOREN had SUBJECT DEVICES 1-4 in his possession at the time he attempted to enter the United States.

9. During a manual review of KOOREN's smartphone (SUBJECT DEVICE 1), Customs and Border Patrol (CBP) discovered a photograph of a prepubescent female

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

sitting down on a chair with an adult male's erect penis in her mouth. CBP alerted HSI, and I responded to conduct further investigation. I viewed the same photo. Based on her small stature and youthful appearance, I estimate the child in this photo is between 5 and 9 years old.

10. I met with KOOREN and identified myself as law enforcement. After obtaining basic biographical information, I asked KOOREN where he had arrived from, the purpose of his travel, and if he had any children. KOOREN told me that he had returned from a trip from the city of Manila in the Philippines, and that he had been there for 3 months visiting his fiancé of 2+ years. He also said he had 2 children who live with their mother. Whan asked, KOOREN could not provide the date of birth for the mother of his children.

11. When asked by SA Orlando what he did for a living, KOOREN stated that he currently was an IT Engineer and had been for the past 17 years.

12. I explained to KOOREN that the reason i was speaking to him was because law enforcement found child pornography on his device. KOOREN asked me if the material were "Border line" or "Very distinct" and if it had come from his "Telegram" folder. I explained that the file was in his phone's files/gallery and assured him it was clearly child sexual abuse material.

13. KOOREN explained that he was a member of a group in Telegram in which other users sometimes attempt to sell Child Pornography but would be kicked out of the group shortly thereafter. He then said that he felt as if he needed an attorney.

14. I told him I had not yet gotten to advising him of his rights but could do so if he wished. He asked me to advise him of his constitutional rights, which I did. KOOREN then asked to speak with a lawyer before answering any further questions. I stopped the interview at that time.

15. I advised KOOREN that because law enforcement discovered child sexual abuse material on his device, I would be seizing all his digital media pending an application for a search warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

16. I took custody of SUBJECT DEVICES 1-4 and placed them in secure evidence storage at the the HSI office in Tacoma, Washington.

17. While I was completing paperwork to leave with KOOREN, he made several spontaneous utterances/statements, including asking if he would be charged in Seattle or North Dakota, stating he understood that all his devices would have to be forensically examined since one one of his devices had child exploitative material on them, and asking if he should get a lawyer in Seattle or North Dakota. I explained to KOOREN that it was not my place to offer legal advice and that those decisions were solely up to him. KOOREN also asked if he was being arrested, and I told him he was not.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

18. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other

19. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Importantly, e-mail and cloud storage can be a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, and possibly reducing the amount of any evidence of any of that material on the users' computer(s).

20. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents, and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

21. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that Harry MATRONE likely has a sexualized interest in children and depictions of children, and that evidence of the commission of the TARGET OFFENSES is therefore likely to be found on the SUBJECT DEVICES.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called "apps," which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. I know from my training and experience that the SUBJECT DEVICES are wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that digital devices and electronic storage media can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device used to access the Internet.] This information can sometimes be recovered with forensic tools.

25. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[2] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate

[2] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

SEARCH TECHNIQUES

27. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICES and will specifically authorize a review of the media or information consistent with the warrant.

28. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES pursuant to this warrant as follows:

a. Securing the Data

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICES.[3]

ii. Law enforcement will only create an image of data physically present on or within the SUBJECT DEVICES. Creating an image of the SUBJECT DEVICES will not result in access to any data physically located elsewhere. However, SUBJECT DEVICES that have previously connected to devices at other locations may contain data from those other locations.

b. Searching the Forensic Images

i. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

ii. For example: These methodologies, techniques, and protocols may include the use of a "hash value" library to exclude normal operating system files that do not need to be further searched. Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results.

---

[3] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

30. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

DANIEL A ORLANDO

Digitally signed by DANIEL A ORLANDO
Date: 2025.03.09 12:25:04 -07'00'

DANIEL A. ORLANDO
Special Agent
Homeland Security Investigations

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 11th day of March 2025.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to be Searched

The SUBJECT DEVICES, currently in the custody of Homeland Security Investigations in secure evidence storage at its office in **Tacoma**, Washington, are described as follows:

One grey Samsung Galaxy S23 FE 128GB, identified by model name: SM-S711U (**SUBJECT DEVICE 1**)

One teal Samsung Galaxy A73, identified by model name: SM-A736B/DS (**SUBJECT DEVICE 2**)

One grey HP Laptop, identified by serial number 5CG0383K3W (**SUBJECT DEVICE 3)**

One Dark grey/black Alienware Laptop, identified by service tag number/serial number HCSVTP2 (**SUBJECT DEVICE 4**)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B
Items to be Seized

The following records on the SUBJECT DEVICES that constitute evidence, fruits, and/or instrumentalities of violation of 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) (the TARGET OFFENSE).:

1. All records relating to violations of the TARGET OFFENSES, including:

a. visual depictions of minors engaged in sexually explicit conduct;

b. identifying information for any individuals depicted in such depictions;

c. information concerning the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct;

d. information identifying the source of any visual depictions of minors engaged in sexually explicit conduct;

e. evidence of communications related to the possession, receive, distribution, or production of visual depictions of minors engaged in sexually explicit conduct;

f. evidence of contact with or communication about minors;

g. evidence related to the sexual abuse or exploitation of minors;

h. i evidence indicative of a sexualized interest in minors or depictions of minors;

2. For each of the SUBJECT DEVICES:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. contextual information necessary to understand the evidence described in this attachment.

3. Records and things evidencing the use of the internet found on the SUBJECT DEVICES, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970